REMARKS

Claims 1-22 are currently pending in the patent application. The Examiner has rejected Claims 3 and 21 under 35 USC 112 as being indefinite. The Examiner concluded that limitations "c" and "d" of Claims 3 and 21 are contradictory and, therefore, indefinite. Applicants respectfully disagree. Limitation "c" recites disconnecting the connection device of the internal basic power supply when a security device is attached to the computer, since the security device comprises the power line of the internal basic power supply. Limitation "d" recites allowing access to the computer when the security device comprises the power line of the internal basic power supply. The connection device secures the power line, as stated in step "b" based on setting data. When the power line is secured by the connection device, the computer cannot be used. However, when the security device is attached as the power line of the internal basic power supply, the connection device is disconnected and access to the computer is allowed. Applicants believe that there is nothing contradictory or indefinite about the limitations. Applicants have, however, amended the claim language to improve the readability thereof. Applicants ask that the Examiner reconsider the rejection based on the foregoing arguments and amendments.

The Examiner has rejected Claims 1-6, 21 and 22 under 35 USC 103 as unpatentable over Miller in view of Kou; and, has rejected Claims 7-20 under 35 USC 103 as unpatentable over Miller and Kou in view of Isaacman. The Examiner had previously indicated, in the ***Response to Arguments*** section, that Applicants had pointed out features of the claimed invention that differ from Miller; but, that the claims did not reflect the differences. Accordingly, Applicants previously amended the claims to more explicitly recite those differences. In response thereto, the Examiner has newly cited the Kou patent. For the reasons set forth below; Applicants believe that all of the claims are allowable over the cited art.

The present invention teaches a method, system, and program storage device for enabling a security function for a computer, wherein a security device is optionally attached to the computer and wherein, when a security device is attached, the use of the computer can be selectively enabled. In a first embodiment of the invention, to which Claims 1, 2, 5, 7, 9, 11, 14, 16, 18, 20 and 22 are directed, a detect enable bit is stored at a first storage location in the computer, wherein the detect enable bit setting designates subsequent processing relative to a security device/function. After the detect enable bit has been set, the computer detects whether a security device is attached and sets an attachment bit in a second storage location of the computer accordingly. The detection can be done continually, when the computer is powered up, or when the computer enters an energy-saving mode. The computer will subsequently use the setting data and attachment data to detect removal of a security device. If a security device has been removed, and the attachment data (a.k.a., the security device history bit) indicates that a security device should be there, access to the computer is prohibited. In a further embodiment of the invention, to which Claims 3, 4, 6, 8, 10, 12, 13, 15, 17, 19 and 21 are directed, the connection of a lithium battery or the like, or the conduction of the power line of the internal basic power supply is carried out based on setting data. This conduction is enabled by connection means such as an analog switch. With this, even for a computer having no security function, the internal basic supply is not shut down. Disconnection is performed when the power line of the internal basic power supply is formed by the security device, and after the security device is once attached and the system recognizes that this computer is a computer having a security function. This is because the internal basic power supply is not disconnected even if the connection is released, since the power line of the internal basic power supply is formed by the security device. If the security device is removed, and if it is unauthorized access to the computer, the power line of the internal basic power supply is disconnected, and the one within the computer which is supplied with power from the internal basic power supply is initialized, so access to the computer is prohibited.

The Miller patent is directed to a system and method for providing a security key device which is not a part of the computer and which must be coupled to the computer bus in order for the computer to be operational. Miller teaches that the security key includes a connector which is coupled to the bus, a controller, and a storage device coupled to the controller. A unique key code is stored in the security key along with an encrypted password. In order for the computer to operate when the security key device is coupled to the computer, the key code stored in the security key must match the key code stored in the computer. Further, a password entered into the computer is encrypted by the security key and must match the encrypted password stored in the security key to enable computer operation.

With specific reference to the claim language, Claim 1 recites a method for prohibiting access to a computer after a security device attached to said computer is removed, comprising the steps of (a) storing setting data comprising a detect enable bit for establishing the computer settings with respect to the attachment of a security device to said computer in a first storage unit of said computer; (b) detecting the attachment of the said security device to said computer after said step (a) and during one of the power-on and the energy-saving mode of said computer; (c) storing the attachment data comprising a security device history bit indicating the detection in step (b) in a second storage unit equipped in said computer; (d) detecting a removal of said security device from said computer based on said previously-stored setting data and said attachment data; and (e) prohibiting access to said computer in response to the detection in said step (d).

With respect to the first step of storing setting data comprising a detect enable bit for establishing the computer settings with respect to the attachment of a security device to the computer in a first storage unit of said computer, the Examiner concludes that the Miller key code obviate the storing of setting data. The Miller security key is not a setting which designates to the computer how to proceed with processing relative to the attachment of a security device. Under the Miller teachings, processing can be conducted in only one way. Miller does not teach or suggest that the process flow can be set differently with respect to a security device. Therefore, the Miller security key does not anticipate or obviate setting data for establishing settings of how the computer will proceed with processing. In fact, Miller expressly states in the Abstract that the connector of the security key ***must*** be coupled to the computer bus for the computer to be operational. Applicants had previously amended the language of independent Claims 1, 5, and 22 to more clearly recite the storing of the setting data and respectfully contend that the amended claim language is not anticipated or obviated by the Miller security key.

With respect to the second claim feature of detecting the attachment of the security device to the computer after storing the setting data and during one of the power-on and the energy-saving mode of said computer, Applicants assert that Miller does not teach the claimed step. The Examiner has stated that the claimed step is "met by comparing the code stored in the security key with the key code stored in the computer". Applicants respectfully assert that a security device must first be detected before a key code from that device can be compared to a key code stored in the computer. Clearly the cited Miller teachings from the Abstract and block 84 of Fig. 5 do not anticipate detecting attachment of a security device during power-on or during entry into an energy-saving mode.

With regard to the claim feature of storing the attachment data comprising the security device history bit indicating detection of attachment of a security device in a second storage unit of the computer, Applicants respectfully disagree with the Examiner's assertion that the claim language is taught by Miller. Miller teaches a key code received from the key 40 being compared to the key code stored in the BIOS flash 24. The key code stored by the computer is stored in one storage location. Whether it is moved into another place for comparison does not change the fact that it is stored in one location. Further, the key code is one value stored at one location. The claim recites a first value, the setting data comprising the detect enable bit, being stored at a first location and a second value, the attachment data comprising the security device history bit, being stored at a second location. Clearly, the Miller patent does not teach or suggest that claim language.

Applicants reiterate that the Examiner has cited the comparison of the key codes against two distinct steps of the present invention. Applicants respectfully assert that the comparing of the key codes cannot anticipate or obviate both a detecting step and a storing step. The Examiner did not respond to this argument in any of the office actions.

With respect to the claim step of detecting removal of the security device from the computer based on the previously-stored setting and attachment data, the Examiner has concluded that Miller teaches that claim language by its illustration in Fig. 7 that, once removal of the security key is detected, the computer is put out of operational mode. The present invention detects that a security device has been removed based on its stored setting data, which tells the computer what attachment-related steps to follow, and based on the stored attachment data, which tells the most recent history of detected attachment of a security device. Miller simply detects the presence or absence of a security device. Miller does not detect ***removal*** of a security device based on previously-stored data. Moreover, Miller simply puts the computer out of operational mode when it detects the absence of a security device. In contrast, the present invention will only execute the step of prohibiting access to the computer if removal is detected, and removal is only detected relative to stored setting data and historical data (Claim 1) or stored setting data and historical data in conjunction with entry of a password (Claim 2). The present invention can grant access if a security device is not there, provided that its stored data indicates that it should not expect to find a security device. The present invention is far more robust that the Miller system.

The Examiner has acknowledged that the Miller patent does not "explicitly teach that computer settings comprising *(sic)* a detect enable bit"; and, has cited the Kou patent. The Kou patent is directed to a system and method for detecting the removal of a removable storage medium in a computer environment. Kou teaches that a predefined control signal (see: Col. 6, lines 10-22) is "shared" between indicating that a removable storage medium has been removed and its "originally established meaning". Further, under Kou, the system receiving the control signal (i.e., an IRQ signal) must then determine the cause of the signal (i.e., whether it is signaling its original purpose or signaling removal of the medium (see: Col. 6, lines 29-37)).

Applicants respectfully disagree with the Examiner's conclusion that "the limitations `a detect enable bit' and 'history bit' are met by IRQ bit". Since Kou teaches that an existing control signal is given an alternate meaning, it is clear that Kou is not providing a specific detect enable bit. Moreover, the present invention claims not only the use of a detect enable bit, but also a separate history bit which is distinct from the detect enable bit. The Kou teaching of having one signal with two different meanings is not the same as or suggestive of the claimed use of two distinct bits for different purposes. Applicants respectfully conclude that the Examiner has not made out a *prima facie* case of obviousness since the cited references do not teach or suggest all of the claim limitations (*In re Wilson*, 424 F. 2d 1382, 165 U.S.P.Q. 494 (C.C.P.A. 1970)).

The Examiner has acknowledged that the combination of Miller and Kou does not teach the use of RFID tags. The Examiner has cited the Isaacman patent as teaching a conventional RFID tag system. Applicants respectfully assert that the additional of the Isaacman RFID teachings to the Miller and Kou patents would not render the pending claims obvious. If one were motivated to include the Isaacman teachings, one would provide an RF antenna as the connector of the security key which would be coupled to the bus of the computer. Such a modification would not result in the invention as claimed, since none of Miller, Kou, or Isaacman teaches or suggests the claim features of storing setting data for setting the attachment of a security device to the computer or of using the setting data in conjunction with detected attachment data for detection of removal of a security device (Claims 1, 2, 5, 7, 9, 11, 14, 16, 18, 20 and 22) or of using the setting data for connecting a connection device of an internal basic power wiring thereby to secure a power supply line (Claims 3, 4, 6, 8, 10, 12, 13, 15, 17, 19, and 21). Applicants respectfully conclude that the Examiner has not made out a *prima facie* case of obviousness since the cited references do not teach or suggest all of the claim limitations (*In re Wilson*, 424 F. 2d 1382, 165 U.S.P.Q. 494 (C.C.P.A. 1970)).

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

H. Horikoshi, et al

By: Anne Vachon Dougherty
Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910